

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA**

IN THE MATTER OF THE SEIZURE OF

FILED UNDER SEAL

- | | | | |
|----|--|---|-----------------------------|
| a. | All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging Claudia NKWENTI, account number 38923124 (“Wallet 2”); |) | Case No. 1:22-MJ- <u>46</u> |
| b. | All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to June NEBA, account number 39757394 (“Wallet 4”); |) | Case No. 1:22-MJ- <u>47</u> |
| c. | All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Stalone MBUNA, account number 55244423 (“Wallet 5”); |) | Case No. 1:22-MJ- <u>48</u> |
| d. | All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Stone AKUM, account number 36959447 (“Wallet 6”); |) | Case No. 1:22-MJ- <u>49</u> |
| e. | All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Aurelie KENMOGNE, account number 13970839 (“Wallet 7”); |) | Case No. 1:22-MJ- <u>50</u> |
| f. | All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Christian NWADISIA, account number 35484558 (“Wallet 8”); |) | Case No. 1:22-MJ- <u>51</u> |
| g. | All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Alain NYONGBELLA, account number 36944333 (“Wallet 9”); |) | Case No. 1:22-MJ- <u>52</u> |
| h. | g. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Cedric FON, account number 35560857 (“Wallet 10”); and |) | Case No. 1:22-MJ- <u>53</u> |
| i. | h. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Wilfred EBOT account number 36674597 (“Wallet 11”). |) | Case No. 1:22-MJ- <u>54</u> |

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT**

I, Joshua T. Tripp, being duly sworn under oath, depose and say:

Introduction

1. I am a Special Agent of the Department of Justice, Drug Enforcement Administration (DEA). As such, I am “an investigative or law enforcement officer of the United States,” as defined within Section 2510(7) of Title 18, United States Code, and empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 21 of the United States Code. I have been employed as a Special Agent with DEA since August 2016. I am currently assigned to the Chattanooga Resident Office, Chattanooga, Tennessee, investigating narcotics trafficking, money laundering, and the diversion of illicit pharmaceutical controlled substances and listed chemicals.

2. I received approximately twenty-four (24) weeks of specialized training in Quantico, Virginia, pertaining to narcotics trafficking, money laundering, undercover operations, and electronic and physical surveillance procedures. I also attended an additional twelve (12) weeks of specialized training as a DEA Diversion Investigator (DI), receiving instruction on investigative techniques on the diversion of pharmaceutical controlled substances and listed chemicals

3. Prior to being a DEA Special Agent, I was a sworn law enforcement officer in the state of North Carolina since 2006. In that capacity, I investigated many violations of North Carolina State Laws, including the North Carolina Controlled Substances Act. As a result, I have become familiar with methods of operation of drug traffickers and organizations. As a Special

Agent with the DEA, I have the responsibility of working with other federal and state law enforcement officers in investigations of violations of federal and state controlled substance laws, including the investigation of heroin, schedule II pharmaceutical pills, cocaine, methamphetamine, marijuana and other dangerous drug organizations.

4. Based on my training, experience and conversations with other experienced narcotics investigators, I have gained experience in the techniques and methods used by drug traffickers to distribute controlled substances, their use of cellular phones and other electronic communication devices to facilitate their trafficking activity, and the methods used to conceal and launder the proceeds of said activity.

5. Through my involvement in a federal Title III investigation, I gained experience in that investigation involving the interception of wire and electronic communications. I have been directly involved in the review and deciphering of intercepted coded conversations between narcotics traffickers that were later corroborated by surveillance. Throughout my law enforcement career, I have spoken with, worked with, and gained knowledge from numerous experienced federal, state, and local narcotics officers about drug traffickers and their use of cell phones to facilitate drug trafficking by, for example, using code during their conversations. I have also received extensive instruction and practical training on intercepting communications and conducting coordinated surveillance while at the DEA Academy

Purpose of Affidavit

6. This affidavit is submitted in support of an application for combined criminal and civil forfeiture seizure warrants for the following assets (collectively, the "SUBJECT WALLETS"):

- a. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Claudia NKWENTI, account number 38923124 (“Wallet 2”);
- b. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to June NEBA, account number 39757394 (“Wallet 4”);
- c. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Stalone MBUNA, account number 55244423 (“Wallet 5”);
- d. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Stone AKUM, account number 36959447 (“Wallet 6”);
- e. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Aurelie KENMOGNE, account number 13970839 (“Wallet 7”);
- f. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Christian NWADISIA, account number 35484558 (“Wallet 8”);
- g. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Alain NYONGBELLA, account number 36944333 (“Wallet 9”);
- h. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Cedric FON, account number 35560857 (“Wallet 10”); and
- i. All funds—including cryptocurrencies—stored in or accessible via the Binance wallet belonging to Wilfred EBOT account number 36674597 (“Wallet 11”).

7. I have been participating in the investigation of shanghaichemicals.com, the website operators, and others for violations of 21 U.S.C. §§ 846, 841(a)(1), 841(b)(1)(A), and 843(b) as well as 18 U.S.C. §§ 1343 and 1956.

8. As set forth below, I submit that there is probable cause to believe that the SUBJECT WALLETS are property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of violations of 21 U.S.C. §§ 841(a)(1) and/or 846 (distribution and possession with intent to distribute a controlled substance), 21 U.S.C. § 843(b) (unlawful use of a communication facility, including the U.S. mails, to facilitate the distribution of a controlled substance), 18 U.S.C. § 1956 (money laundering), and 18 U.S.C. § 1343 (wire fraud).

9. Because this affidavit is submitted for the limited purpose of obtaining warrants authorizing the seizure of the SUBJECT WALLETS, I am not including every fact known to me about the defendants or the larger investigation.

10. This affidavit is based upon my own personal observations, my training and experience, discussions with other agents who are familiar with this investigation, and information collected during this investigation through, among other things, witness interviews, law enforcement investigation reports, information obtained through searches, and public records.

Background on Cryptocurrency

11. Cryptocurrency (also known as digital currency) is generally defined as an electronically sourced unit of value that can be purchased with, sold for, or used as a substitute for fiat currency (*i.e.*, currency created and regulated by a government). Cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Cryptocurrency is not illegal in the United States.

12. Bitcoin (“BTC”), Bitcoin Cash (“BCH”), Litecoin (“LTC”), and Ethereum (“ETH” or “ether”) are some common types of cryptocurrencies. Payments made with these cryptocurrencies are recorded in a public ledger that is maintained by peer-to-peer verification

(*i.e.*, a “blockchain”) and is thus not maintained by a single administrator or entity. Cryptocurrencies are widely used to conduct both legitimate and illegitimate business. For example, Microsoft accepts bitcoins as payment for Xbox games and services. On the other hand, bitcoins were the payment method used on Silk Road and Dream Market, websites on the dark web that offered drugs and other contraband for sale.

13. Individuals can acquire bitcoins, bitcoin cash, litecoins, and ether through, for example, exchanges (*i.e.*, websites—such as Coinbase, which is described further below—that allow individuals to purchase or sell cryptocurrencies in exchange for fiat currency or other cryptocurrencies), ATMs, or directly from other people. Binance is one such cryptocurrency exchange. According to Binance’s website, it is the “world’s largest crypto exchange.”

14. Individuals can also acquire cryptocurrencies by “mining.” An individual can mine bitcoins, bitcoin cash, litecoins, and ether by allowing his/her computing power to verify and record payments into the aforementioned public ledger. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency.

15. Individuals can send and receive cryptocurrencies through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on many types of computers, including laptop computers and smart phones.

16. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a public ledger, the true identities of the individuals or entities behind the public addresses are not recorded on the public ledger. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin, Bitcoin Cash, Litecoin, and Ethereum-based transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous.

17. Bitcoins, bitcoin cash, litecoins, and ether can be stored in digital “wallets.” A wallet essentially stores the access code that allows an individual to conduct cryptocurrency transactions on the public ledger. To conduct transactions on the public ledger, an individual must use a public address (or “public key”) and a private address (or “private key”). The public address can be analogized to a traditional bank account number, while the private key is like the password or PIN used to access that bank account.

18. Exchangers and users of bitcoins, bitcoin cash, litecoins, and ether often store, and transact with, these cryptocurrencies in several ways, utilizing desktop, mobile, and online wallets; hardware devices; and paper wallets. Desktop, mobile, and online wallets are electronic in nature and can be stored on mobile devices (e.g., smart phones or tablets) or websites that users can access via a computer, smart phone, or any device that can search the internet. Wallets can also be stored on external or removable media and hardware (such as USB thumb drives). In addition, paper wallets contain an address and a QR code¹ with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “seed phrase” (random words strung together in a phrase, also known as a “recovery phrase”) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that the cryptocurrencies become potentially vulnerable to seizure and/or unauthorized transfer.

¹ A QR code is a matrix barcode that is a machine-readable optical label.

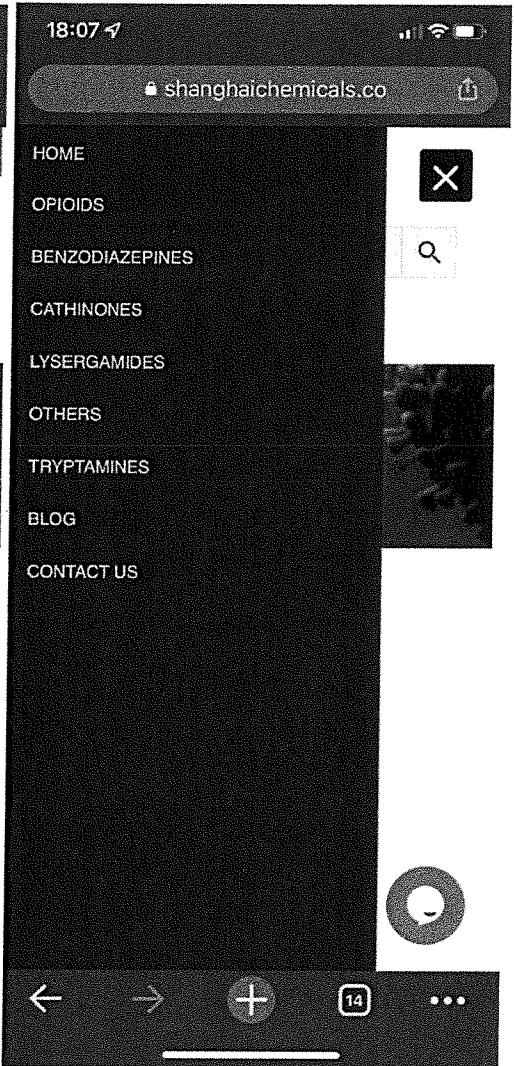
Summary of the Investigation

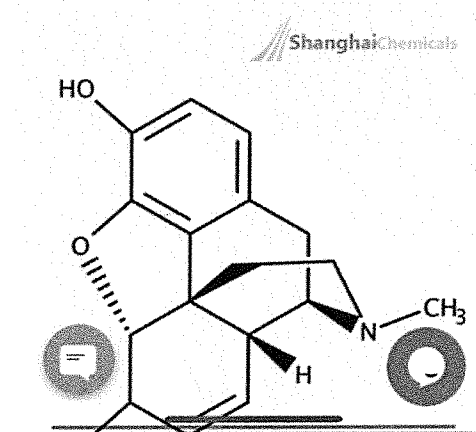
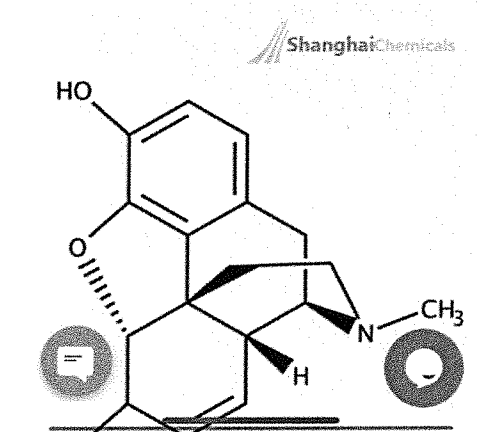
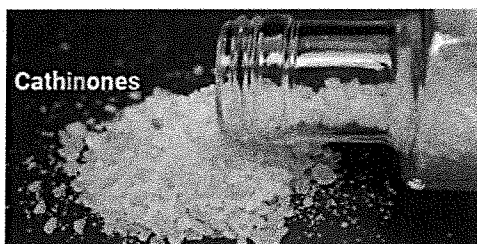
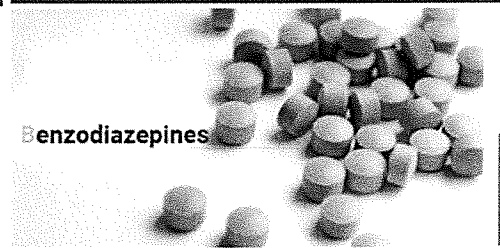
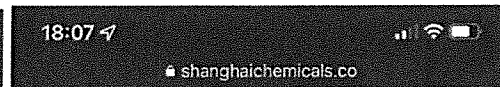
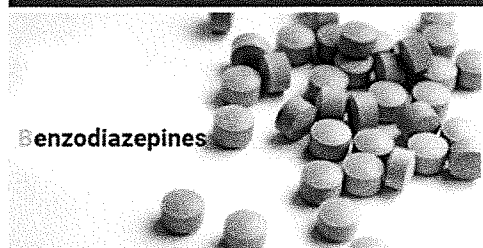
19. The United States, through the Drug Enforcement Administration and coordinating agencies and offices, is investigating the distribution of controlled substances in and around the Eastern District of Tennessee. The investigation concerns possible violations of 21 U.S.C. §§ 841, 843, 846 and 18 U.S.C. §§ 1343 and 1956.

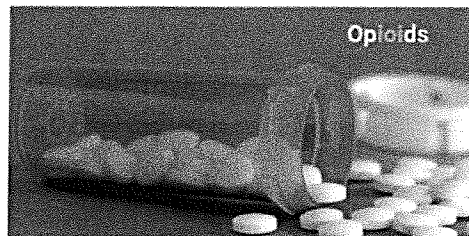
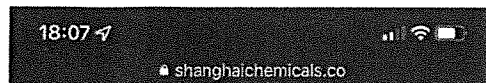
20. I and other federal law enforcement personnel are engaged in the investigation of drug trafficking occurring in and around the Eastern District of Tennessee, via website “shanghaichemicals.co.”

21. Investigators with DEA Chattanooga, DEA Beijing, and Homeland Security Investigation (“HSI”) Beijing have been investigating the distribution of fentanyl in Chattanooga, Tennessee and elsewhere. During the course of the investigation, an HSI confidential source (“CS”) informed investigators that a website operating on the Clearnet (i.e., the indexed internet accessible through publicly available browsers) – shanghaichemicals.co – was distributing fentanyl worldwide.

22. Investigators reviewed the website shanghaichemicals.co and found that the website advertises multiple controlled substances for sale including but not limited to: opioids, benzodiazepines, cathinones, lysergmides, and tryptamines. Investigators found that the website allows for the purchase of these items without a prescription. The website indicates that the company is located in Beijing, China. However, investigators found that the website is hosted by Namecheap, a domain name registrar and web host based in Phoenix, Arizona. Other than advertising disposable masks and gloves for sale, it appears that shanghaichemicals.co is a website entirely dedicated to the illegal distribution of controlled substances. For example, screenshots of the website include:

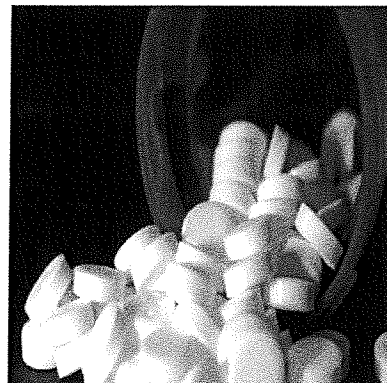
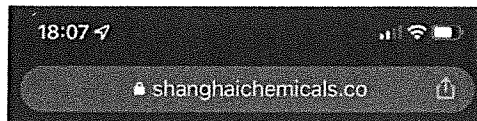






Today Offer: \$20 OFF orders \$300 or more with code "Shanghaichemicals" + Free shipping on orders over \$60! Offer Details

LATEST PRODUCTS

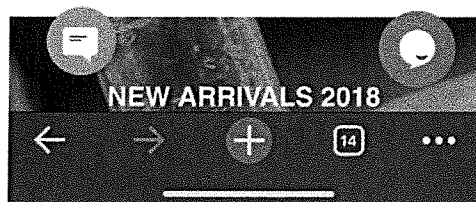


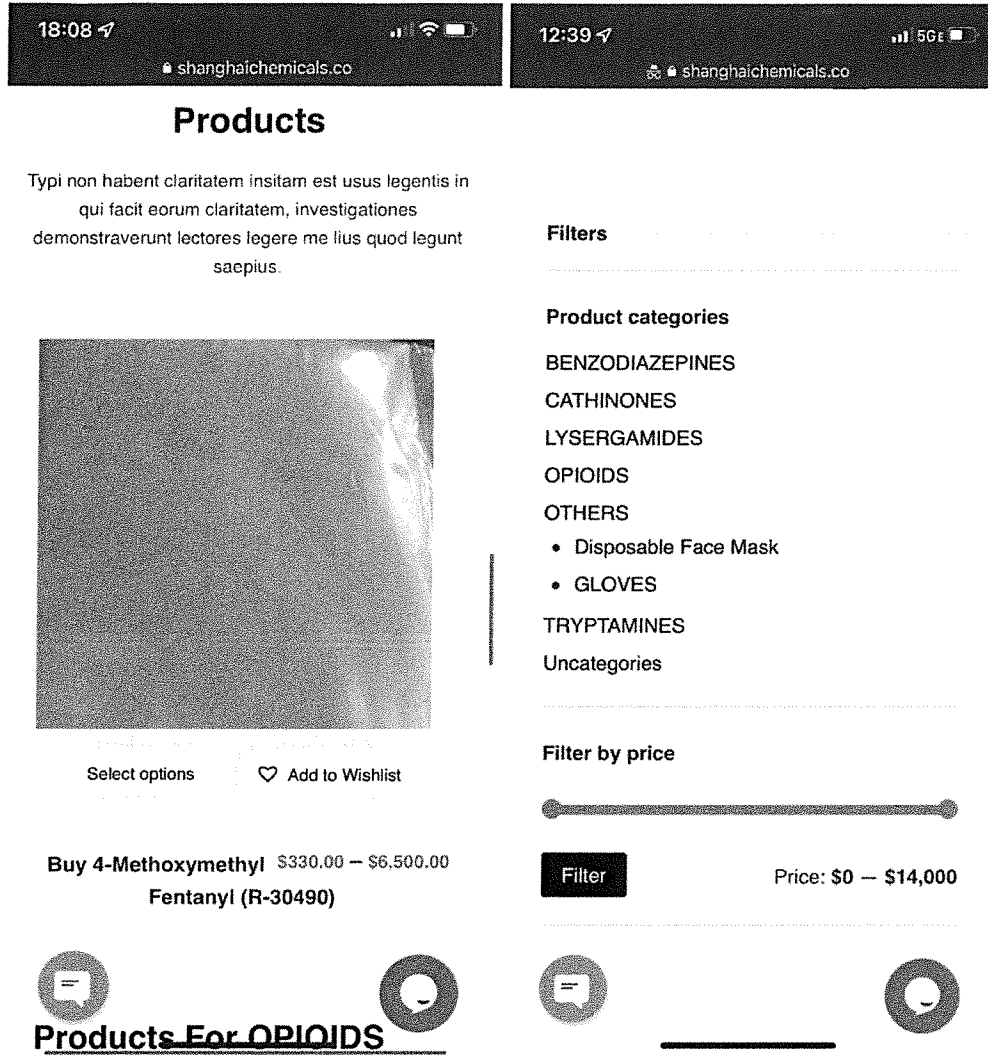
Add to cart

Add to Wishlist

Morphine

\$125.00



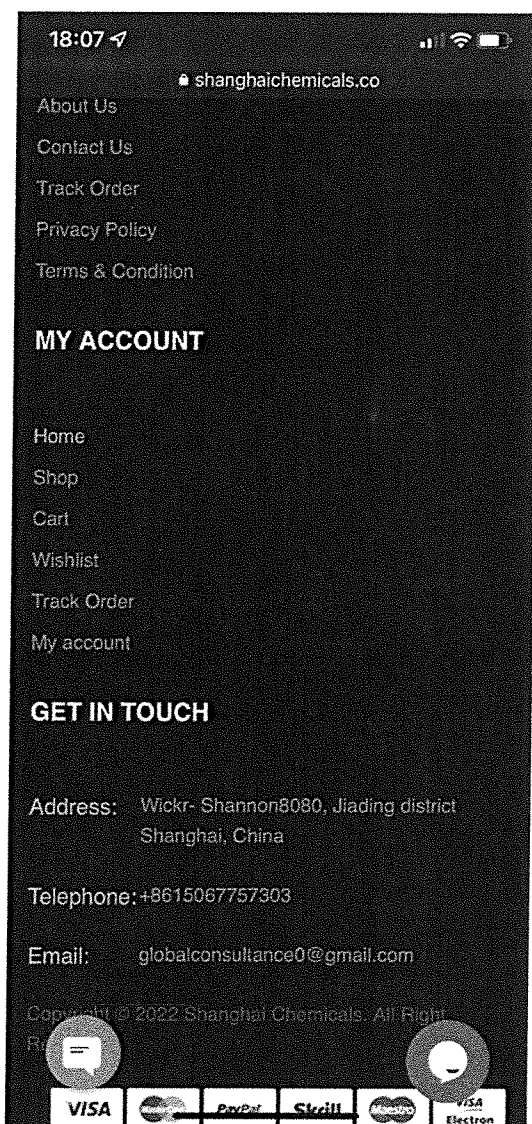


23. Investigators found that the website lists a Wickr² handle of “Shannon8080”³ as a contact point for users to “GET IN TOUCH.” Under the same “GET IN TOUCH” heading, the website also lists email address “globalconsultance0@gmail.com,” and WhatsApp phone number, “+86 15067757303.” WhatsApp is a cross-platform phone messaging application that allows users

² Wickr is an end-to-end encrypted messaging application.

³ Shannon8030 appears to be a pseudonymous moniker.

to send and receive text messages and voice calls. In my training and experience, I know that drug traffickers commonly use WhatsApp to further their drug trafficking operation. WhatsApp communication is secure and encrypted, which thwarts law enforcement investigative efforts.



24. Investigators found that shanghaichemicals.co was registered to the name “Wickr Shannon” with email address globalconsultance0@gmail.com, and phone number +86 1506775703.

25. According to access logs for the Namecheap account affiliated with the operator of shanghaichemicals.co, the IP addresses accessing the website appear to belong to Virtual Private Networks (“VPNs”).⁴ In my training and experience, I know that criminals use VPNs and other anonymizing methodologies to conceal their true IP address and attempt to avoid detection. I believe that the account information related to the name of the account holder is fictitious and that it closely resembles the advertised Wickr moniker. Through my training and experience, I know it is common for bad actors to use fictitious names and monikers while conducting business online. This allows the individual(s) to conceal their identity to thwart law enforcement efforts.

26. In October 2021, investigators instructed the CS to contact Shannon8080 and order 130 grams of fentanyl from Shannon8080. The CS and Shannon8080 communicated via the Wickr application using the information featured on the website shanghaichemicals.co. Through that conversation, Shannon8080 told the CS that the CS could order 130 grams of fentanyl from Beijing, China, to the United States for \$2,499.00. Shannon8080 further directed the CS to deposit the money into a US bank account at Branch, Bank and Trust (“BB&T”) (now owned by Truist Bank). Shannon8080 provided the CS with the bank account number ending in 9276 in the name of Belinda Carroll (hereinafter “designated bank account”).

27. In October 2021, the undersigned, working in an undercover (“UC”) capacity, deposited \$2,499.00 into the designated bank account located in Chattanooga, Tennessee. The purpose of that deposit was for the account holder of the designated bank account to transfer the money to Shannon8080 in exchange for the fentanyl shipment to Chattanooga, Tennessee.

⁴ VPNs are a method of establishing a private network connection between devices. Effectively, this means that a user is accessing computers through the internet using an IP address that is not, in fact, the IP address assigned to that user’s home network.

28. Shannon8080 told the CS, via Wickr, that the money had been received into the designated bank account and that the fentanyl was being processed for shipment. However, Shannon8080 later told the CS that the US bank account holder converted the US currency (“USD”) to Bitcoin (“BTC”) and that, during the conversion, the \$2,499.00 USD was reduced to \$1,550.00 USD. Shannon8080 told the CS that the processing would stop unless the CS deposited an additional \$790.00 USD. The CS negotiated the new asking price down from \$790.00 to \$500.00 USD, to which Shannon8080 agreed.

29. To facilitate the additional \$500 payment, on November 3, 2021, the undersigned, again working in a UC capacity, contacted Shannon8080 through Wickr. Shannon8080 provided UC with a BTC wallet address, bc1qwa... (“Wallet 1”),⁵ and confirmed that the 130 grams of fentanyl would ship to UC after the BTC deposit to Wallet 1 was received. Shannon8080 told UC that after the BTC deposit was confirmed, a tracking number would be provided within twenty-four (24) hours.

30. Per Shannon8080’s instructions, on November 8, 2021, the UC transferred 0.00770000 Bitcoin from his UC wallet to Wallet 1. After completing the transfer, records show that the UC funds from Wallet 1 were transferred into two other wallets, 1FMDLn... (“Wallet 2”) and bc1q7x... (“Wallet 3”). Wallet 2 is a Bitcoin wallet owned by Claudia Bimu NKWENTI on the Binance exchange, account number 38923124. Wallet 3 has no personal identification

⁵ Given the length and complexity of the wallet addresses herein, this Affidavit references the first six characters of the wallet address followed by an assigned sobriquet (e.g., “Wallet 1”).

information available. On November 9, 2021, Wallet 3 transferred the UC funds received from Wallet 1 into Wallet 2.⁶

31. In November 2021, the undersigned received information pertaining to the email address listed as a contact for shanghaichemicals.co, globalconsultance0@gmail.com. Access logs for globalconsultance0@gmail.com indicate that from October 2021 to November 2021, globalconsultance0@gmail.com was accessed over 15,000 of times by various IP addresses.

32. On November 10, 2021, the undersigned, again acting in an undercover capacity sent an e-mail to globalconsultance0@gmail.com. The email inquired about the UC order of 100 grams of fentanyl. As of the date of application for this warrant, UC has not received a reply from that e-mail address about the fentanyl.

33. Further investigations revealed that that Claudia NKWENTI, the named holder of Wallet 2, is a Cameroon National who has applied for a U.S. Visa. That application was denied by the Department of State due to concerns of overstaying and “weak ties to Cameroon.” Claudia NKWENTI’s sister, Edna NKWENTI is a legal permanent resident of the United States and resides in Oakley, California.

34. In February 2022, Binance provided records related to Wallet 2, including access logs to the account belonging to Claudia NKWENTI. Those access logs provided IP addresses for each access to the account. Investigators determined that there were eighteen (18) identical IP addresses accessing both the globalconsultance0@gmail.com email account and Claudia NKWENTI’s Binance account.

⁶ After this transfer, Wallet 2 was in possession of all \$500.00 of the UC funds that were originally transferred into Wallet 1.

35. A review of records pertaining to Wallet 2 revealed that from February 2021 to November 2021, there were approximately 4,878 deposits into Wallet 2, totaling nearly 76.52241178 Bitcoin⁷. Further, from March 2021 to November 2021, there were 759 withdrawals from Wallet 2 to other wallet addresses totaling approximately \$3,575,238.71 worth of cryptocurrencies. Further review into Wallet 2 revealed that hundreds of the deposits were made in the cryptocurrency Bitcoin. After receiving the Bitcoin, the user converted the Bitcoin to Tether (“USDT”).⁸ After the conversion, USDT was transferred from Wallet 2 to other cryptocurrency wallets. I know that cryptocurrency is often converted from one currency to another in an effort to conceal and launder money. Cryptocurrency also transferred quickly after its form is converted to further conceal and launder money.

36. Between November 8 and 11, 2021, in addition to the funds received from Wallet 1 that the UC first deposited, Wallet 2 received 130 deposits totaling 2.1059897 Bitcoin. According to Binance records, Wallet 2 receives several deposit and withdrawal transactions each day. Those deposits are similar in amount to the Bitcoin deposited by the UC for the purchase of fentanyl. Investigators believe that the deposits are from other orders of illicit narcotics from the website, shanghaichemicals.co. After the Bitcoin was deposited, consistent with laundering techniques, it was quickly converted to USDT and withdrawn and transferred to other accounts.

⁷ As of February 2, 2022, Bitcoin was valued at \$37,478.60, down from the all-time high of about \$68,000.00 in November 2021.

⁸ Tether is a cryptocurrency that is hosted on the Ethereum and Tron blockchains. Tether has a 1:1 equivalent to the US Dollar.

37. According to Binance records, on November 8, 2021, Wallet 2 converted the funds received from Wallet 1 to USDT, which included the Bitcoin deposited by undersigned while working in an undercover capacity.

38. Investigators found that Wallet 2 co-mingled the original 0.00770000 Bitcoin received from Wallet 1 with other funds received. After co-mingling the funds and converting Bitcoin to USDT, Wallet 2 withdrew USDT from Wallet 2 on multiple occasions and transferred the proceeds to other cryptocurrency wallets. Between November 8 to November 12, 2021, Wallet 2 withdrew 115,491.08 USDT, transferring it into 19 other cryptocurrency wallets. Of those 19 wallet addresses, eight (8) wallets were managed by Binance.⁹

39. One of the Binance wallets that Wallet 2 transferred USDT in to was THM7Z2... (“Wallet 4”). Binance Wallet 4 is owned by Jude NEBA and managed by Binance, account number 39757394. Jude NEBA is a Cameroon national. Jude NEBA has applied for a US Visa, but was denied due to concerns about a possible overstay and weak ties to the Cameroon. June NEBA has a cousin, Emelda SIRRINGWEN, who lives in Otsego, Minnesota.

40. According to Binance records, Wallet 4 maintains approximately \$27,287.00 worth of cryptocurrency as of January 2022; given fluctuations in value of cryptocurrency, the dollar-equivalent value of the wallet varies daily according to the market price of the cryptocurrency. According to blockchain analysis, Wallet 4 made 8,783 transactions between March 21, 2020, and January 4, 2022. Those transactions total approximately \$37,998,598.78 worth of cryptocurrency.

⁹ This Affidavit references a wallet “managed by Binance,” meaning, in this context, that it is a web-based wallet controlled by a user, but accessible and operated through the Binance online platform.

41. Investigators also received access log information for Jude NEBA's Binance account. Those access logs contained the IP addresses that were accessing Jude NEBA's Binance account. Investigators found that twenty-two (22) of the IP addresses that accessed the email account globalconsultance0@gmail.com (i.e., the e-mail listed as contact info for the operators of the drug-dealing website shanghaichemicals.co) also accessed Jude NEBA's Binance account (Wallet 4). Of those 22 IP addresses, twelve (12) also accessed Claudia NKWENTI's Binance account (Wallet 2).

42. Investigators also reviewed other Binance accounts into which Wallet 2 transferred cryptocurrency between March 11, 2021, and November 12, 2021. Investigators identified the following wallets as receiving funds from Wallet 2: TKtUf8...("Wallet 5"), a Binance account owned by Christian NWADISIA, account number 35484558; TNDKTL...("Wallet 6"), a Binance account owned by Aurelie KENMOGNE, account number 13970839; TVp2a7...("Wallet 7"), a Binance account owned by Wilfred EBOT, account number 36674597; TErv5i... ("Wallet 8"), a Binance account owned by Stone AKUM; account number 36959447, TXW7P... ("Wallet 9"), a Binance account owned by Stalone MBUNA account number 55244423; TPZ2F... ("Wallet 10"), a Binance account owned by Alain NYONGBELLA, account number 36944333; and TJeevu... ("Wallet 11"), a Binance account owned by Cedric FON, account number 35560857. (See Attachment A for illustration).

43. The analysis conducted on Wallets 5 through 11 revealed that each of the accounts conducted numerous transactions beginning around December 2017 and continuing through January 2022. In total the aforementioned accounts conducted 77,573 transactions that totaled approximately \$448,812,212.08 USD worth of cryptocurrency transactions.

44. The below graph illustrates the total amount of cryptocurrency and its USD equivalent that is contained within each of the accounts, i.e., the account's current balance as of January 3, 2022:

Account / Currency	Estimated Value	BTC	Estimated USD Value
AURELIE CHRISTELLE DJOKO KENMOGNE	1		\$60,306.00
CHRISTIAN UCHECHUKWU NWADISIA	2		\$57,543.00
WILFRED BESON EBOT	1		\$51,804.00
JUDE AMBE NEBA	1		\$27,287.00
ALAIN TADOH NYONGBELLA	0		\$8,598.00
STONE WENJERI AKUM	0		\$2,718.00
STALONE NKEMBENG MBUNA	0		\$1,090.00
CEDRIC TIFUH FON	0		\$5.00
Grand Total	5		\$209,351.00

45. Investigators reviewed access logs for each of accounts affiliated with Wallets 4 through 11. IP addresses accessing the globalconsultance0@gmail.com email address (i.e., the e-mail listed as contact info for the operators of the drug-dealing website shanghaichemicals.co) were also accessing each of the Binance accounts, that is Wallets 4 through 11, with one exception, the Binance account belonging to Christian NWADISIA (Wallet 5). However, investigators found that many of the IP addresses accessing Wallet 5 were also accessing all of the aforementioned Binance accounts, that is Wallet 4, and Wallets 5 through 11.

46. On February 11, 2022, I received and reviewed access logs related to the WhatsApp, number, 86 15067757303, the number listed in the "GET IN TOUCH" section of the website. WhatsApp is a cross-platform centralized instance messaging and voice-over-IP (VOIP)

service that allows text messages, voice messages, and video calls. I found multiple IP addresses accessing the WhatsApp account, were also accessing the email address, “globalconsultance0@gmail.com” and some of the Binance wallet accounts.

47. Based on IP address patterns and access activity, it appears that a common source is acting as the “GET IN TOUCH” contact advertised by the drug-dealing website shanghaichemicals.co and accessing and controlling the wallets described herein. Additionally, investigators found that many of the IP addresses that are accessing the aforementioned Binance wallets are also accessing other Binance and Coinbase exchange accounts.

48. The SUBJECT WALLETS associated with the cryptocurrency addresses identified in Attachment A are held in Binance Holdings Limited, located in Grand Cayman, Cayman Islands.

49. In my training and experience, I believe that the SUBJECT WALLETS are conducting activity associated with money laundering. The pattern of withdrawals, transfers, and transactions is consistent with money laundering and attempts to conceal drug proceeds. Further, cryptocurrency is frequently used by criminals operating in the digital sphere as a medium of money laundering due to its pseudonymity and the perceived difficulties in tracing funds. I have conferred with Binance investigators who stated that it is common for money launderers to obtain Bitcoin and immediately convert the funds to another cryptocurrency, such as USDT, and to transfer to multiple other accounts in order to attempt to “wash” the money and hide illicit funds.

50. Bad actors sometimes utilize services to further obfuscate the movement of funds. A cryptocurrency tumbler or cryptocurrency mixing service is a service that mixes cryptocurrency funds with funds belonging to other individuals, so as to obscure the trail back to the fund's original

source. When cryptocurrencies are tumbled or mixed, the mixer will take the cryptocurrency from several different users and run them through an algorithm that mixes those funds together, and then redistributes them to the users. For example, one hundred users send 0.1 bitcoin to a new address, aggregating those funds into one big transaction. The funds are subsequently distributed among the hundred users, each of them receiving 0.1 “clean” bitcoin. As a result, tumbled or mixed cryptocurrencies lose many of the attributes that make cryptocurrencies traceable. There does not appear to be a legitimate reason for this type of activity. The conversion to USDT creates a 1:1 ratio to the US Dollar. After converting the USDT, the accounts transfer to several other accounts without withdrawing the funds.

51. It is also possible for owners of cryptocurrencies to exchange or covert one cryptocurrency to another (i.e.: converting Bitcoin to Tether) and then sending the new cryptocurrency to other wallet addresses. Converting and sending the cryptocurrency to other wallets thwarts investigator’s ability to trace the movement of funds.

52. In this case, Wallet 2 and other SUBJECT WALLETS received funds obtained by virtual currency transfers that occurred after an attempted undercover purchase of fentanyl. During that transaction, UC investigators transferred Bitcoin to a wallet address provided by an unknown co-conspirator. After the transaction, the funds were transferred to another virtual currency wallet owned by Claudia NKWENTI in Wallet 2. Wallet 2 then converted the Bitcoin to USDT and transferred that virtual currency to multiple other wallet addresses, owned by other individuals. While reviewing the Binance account for Claudia NKWENTI, investigators found thousands of deposits from February 2021 through November 2021. All of the deposits were in Bitcoin and all were for amounts ranging from a few hundred dollars to a few thousand dollars. These amounts are similar to what the amount would be if a customer purchased the products listed on

shanghaichemicals.co. Investigators found over 5,000 of such deposits into the wallet. These small deposits totaled approximately 76.52 Bitcoin, which as of February 9, 2022 is approximately \$3,398,888.32 USD. Law enforcement placed a UC order of drugs advertised on the website shanghaichemicals.co and sent funds to Wallet 2 at the website operators' instruction; however, law enforcement never received the drugs that were ordered and paid for. Accordingly, I believe that, in addition to the potential sale of illicit narcotics, this website may be involved in fraudulent activity, i.e., advertising drugs for sale, accepting payment for the notional drugs, but never sending the product ordered.

53. Insofar as criminal forfeiture is concerned, I know that a protective order would be inadequate to ensure the preservation of the funds in the above-listed wallets because funds stored electronically can be easily and almost instantaneously transferred from remote locations, and that financial institutions and those that hold cryptocurrency do not always act promptly to make all of their employees are aware of restraints that are placed on such funds. Moreover, the unique nature of cryptocurrency makes transfer of funds available instantaneously. Courts have routinely issued seizure warrants, rather than restraining orders, in cases where the property was highly fungible. It is the nature of the property itself which is sufficient for the court to find that a restraining order may be inadequate. *United States v. Swenson*, 2013 WL 3322632 (D. Idaho July 1, 2013) (the court is entitled to infer from the inherent fungibility and transferability of money in a bank account that a restraining order would be inadequate); *United States v. Lewis*, 2006 WL 1579855, *5 (D. Minn. June 1, 2006) (vehicles and funds in a bank account may be seized pursuant to section 853(f) because both can easily be moved or transferred; a restraining order would be inadequate); *United States v. Wiese*, 2012 WL 43369, *2 (E.D. Mich. Jan. 9, 2012) (§ 853(f) warrant may be used to seize funds in a bank account because they may be easily moved);

United States v. Martin, 460 F. Supp. 2d 669, 667 (D. Md. 2006) (finding probable cause to believe that a restraining order would not have been adequate to maintain fungible, transferable property such as cash or money seized from a bank account), *aff'd* 662 F.3d. 301, 304 n.6 (4th Cir. 2011). Moreover, I also know that a restraining order can be violated with ease and that there is no guarantee that a restraining order will prevent the dissipation of the asset.

54. Moreover, with respect to civil forfeiture of fungible property, such as funds deposited in an account at a financial institution, I know that it is unnecessary “for the Government to identify the specific property involved in the offense that is the basis for the forfeiture; and that any identical property found in the same place or account as the property involved in the offense that is the basis for the forfeiture shall be subject to forfeiture.” 18 U.S.C. § 984. With respect to tracing, it is not a defense that the property involved in the offense underlying the basis of forfeiture has been removed and replaced by identical property. 18 U.S.C. § 984(a)(2), so long as the United States commences a civil forfeiture action within a year of the offense. 18 U.S.C. § 984(a)(2).

55. For the drug violations, SUBJECT WALLETS are subject to seizure to the United States pursuant to 18 U.S.C. §§ 981(b) by 21 U.S.C. § 881(b) and 21 U.S.C. §§ 853(e) and (f) and forfeiture pursuant to 21 U.S.C. §§ 853 and 881(a)(6) on the grounds that information provided in this affidavit shows there is probable cause to believe that the funds contained in the above-listed accounts constitute proceeds that are directly traceable to violations of 21 U.S.C. §§ 846, 841 and 843. The SUBJECT WALLETS are further subject to seizure to United States, in accordance with the money laundering violations, pursuant to 18 U.S.C. § 981(b), and 21 U.S.C. §§ 853(e) and (f) by 18 U.S.C. § 982(b)(1) and forfeiture pursuant to 18 U.S.C. §§ 982(a)(1), 981(a)(1)(C) and 981(a)(1)(A), on the grounds that there is probable cause to believe the funds contained in the above-listed accounts constitute proceeds that are directly traceable to violations of 18 U.S.C.

§ 1956. Further, said funds are subject to seizure as they are involved in the violation of 18 U.S.C. § 1956. The SUBJECT WALLETS are subject to seizure to United States, in accordance with wire fraud violations, pursuant to 18 U.S.C. § 981(b), 21 U.S.C. §§ 853(e) and (f) by 18 U.S.C. § 982(b)(1) and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) on the grounds that there is probable cause to believe the funds contained in the above-listed accounts constitute proceeds or are derived from proceeds traceable to violations of 18 U.S.C. § 1343.

56. For the reasons set forth above, probable cause exists to seize the properties. As such, the United States seeks the issuance of warrants providing seizures of the contents of the SUBJECT WALLETS that contain funds constituting proceeds or are traceable to proceeds of drug trafficking, constitute funds involved in or traceable to money laundering violations, and constitute or are derived from proceeds traceable to wire fraud.

57. I submit there is probable cause to believe that these accounts contain proceeds of the crimes listed and detailed above. The events described herein, and the location of the properties in question occurred and are situated in the Eastern District of Tennessee and elsewhere. Accordingly, pursuant to 18 U.S.C. § 981(b)(1)(3), “a seizure warrant may be issued . . . by a judicial officer in any district in which the forfeiture action against the property may be filed under section 1355(b) of Title 28, and may be executed in any district in which the property is found.” 18 U.S.C. § 981(b)(3).

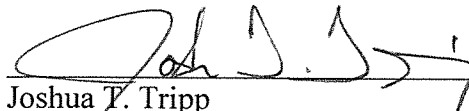
Conclusion

58. Based upon the evidence gathered in this investigation and set out above, I submit that there is probable cause to believe that the SUBJECT WALLETS are subject to civil seizure of the property pursuant to 18 U.S.C. § 981(b) by 21 U.S.C. § 881(b) and criminal seizure pursuant to 21 U.S.C. § 853(e) and (f) and 18 U.S.C. § 982(b)(1). Further, the SUBJECT WALLETS are

subject to civil forfeiture of the property pursuant to 21 U.S.C. § 881(a)(6), 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1), 981(a)(1)(C) and 28 U.S.C. § 2461(c), and 21 U.S.C. § 853.


FURTHER AFFIANT SAYETH NAUGHT.

Executed this _____ day of February, 2022, in Chattanooga, Tennessee,
Located within the Eastern District of Tennessee.



Joshua T. Tripp
Special Agent
Drug Enforcement Administration

Subscribed and sworn to me before
On this 15th day of February, 2022.



Christopher H. Steger
United States Magistrate Judge

Attachment A

Location of subjects on this chart is not based upon hierarchy, this chart simply shows the transactions between accounts.

